# Industry Perspective: Cross Border Privacy Rules (CBPR) System

**SGTech** Advocacy Paper for the APEC Business Advisory Council

ABAC Singapore | April 2023

Written by: Sukaasini Latch, SGTech

# Contents

# Executive Summary

APEC economies developed the Cross-Border Privacy Rules (CBPR) system in 2011 which establishes enforceable, binding commitments to safeguard consumers' personal information when transferring personal data across borders. The CBPR enables companies to certify compliance with commonly agreed rules, i.e. 50 specific program requirements based on the **APEC Privacy Framework**. APEC economies, data privacy regulators, and related stakeholders have been exploring ways to boost the uptake of the CBPR system.

In 2022, ABAC Singapore, as Co-Chair of the ABAC Digital Working Group set out to understand the factors contributing to the low take-up rate of the CBPR system amongst companies and posit industry recommendations to boost CBPR uptake. To that end, ABAC Singapore had one-on-one consultations with companies, and commissioned a survey amongst ABAC and partner networks to gauge the level of awareness and business perception around trust marks[1] and the CBPR, and recognise the impediments faced by businesses to adopt certifications and trust marks, including the CBPR. Singapore also convened a closed-door roundtable with ABAC and partners. Participants engaged in a frank and dynamic discussion to understand business interest and perception of trust marks and privacy certifications such as the CBPR in the region, and identify opportunities for businesses, both big and small to overcome the challenges towards adopting high quality data privacy standards and certifications such as the CBPR.

At the industry level, **lack of interest to adopt the CBPR was attributed to several reasons** which included: (i) low levels of awareness and understanding of CBPR and its requirements; (ii) low levels of participation, resulting in a limited pool of economies and firms' participation and recognition of the CBPR; (iii) fragmented regulatory landscape limiting the recognition of CBPR by regulators within and outside of APEC; (iv) insignificant client demand and recognition of CBPR as a necessary or adequate mechanism and (v) cost of certification being prohibitive to MSMEs.

To enhance CBPR adoption, it was apparent that governments needed to back the CBPR in a strong, vocal manner to get industry's attention and support behind the system. It was also key to build a strong business case to incentivise firms to take up the voluntary certification. In that regard, **top industry recommendations** to improve CBPR uptake included: (i) increasing APEC and non-APEC economies' participation and recognition of the CBPR; (ii) investing in education and awareness building of the CBPR amongst various stakeholders such as governments, regulators, firms, consumers, academia and civil society; (iii) foster greater interoperability and harmonisation of privacy frameworks regionally and globally; and (iv) make CBPR affordable and accessible to MSMEs.

Enhancing the CBPR system requires **strong multi-stakeholder partnerships**, with the private sector being a key stakeholder to the process given that firms are the main users of the CBPR. In that regard, there needs to be an established avenue for regular, robust dialogue between government, industry, academia and civil society to develop targeted action plans and initiatives. In addition to general awareness campaigns, governments and businesses could benefit from regular closed-door, focused group consultations and capacity building

[1] Trust marks here refer to any domestic, regional, or international enterprise-wide certifications that organisations can adopt/apply for to demonstrate that they have adopted sound data protection practices to help strengthen trust with organisations' customers, business partners and regulators.

initiatives to identify and overcome gaps in the capabilities and functions required to improve privacy regimes. This is where international advocacy platforms such as ABAC and local industry associations could play a particularly important role in serving as the bridge to **facilitate partnerships and dialogue** between stakeholders. **Joint advocacy efforts** and **adequate resourcing** will also be essential to move the needle in this regard.

# Introduction

For many companies in the APEC region, cross border data transfers are an integral part of operations (although these data transfers do not necessarily include personal data). With the pervasiveness and exponential growth of the digital economy, the scale and extent of cross border data flows are only set to increase.

In the current operating landscape, common issues that companies face in the transfer of personal data across borders include:

i) Having to adapt to the ever changing data regulatory landscape in economies;
ii) Navigating an often-complex set of domestic requirements and legislation for data transfer;
iii) Being subjected to conditional data transfer requirements (including sectoral restrictions);
iv) Existing certifications not being recognized by the personal data receiving economy to demonstrate compliance

To overcome such challenges, and to protect personal data when facilitating cross border transfers, companies have adopted various approaches (contractual agreements, adopt relevant certifications and standards (such as ISO certifications and standards), to ensure compliance with key regulations, etc.). When assessing and adopting appropriate mechanism(s), the **underlying motivations** come down to key business management considerations, i.e.:

i) Effectiveness of mechanism(s) to demonstrate regulatory compliance;
ii) Ability for mechanism(s) to meet requirement of clients and consumers;
iii) Build trust and credibility amongst clients and business networks with regard to the company's products and services that involve cross border transfer of personal data flows;
iv) Facilitate seamless intra-group organizational personal data transfer flows.

As such, this begs the question as to whether **the Cross Border Privacy Rules (CBPR) system serves as an effective and adequate mechanism** to help facilitate seamless flows of cross border transfers of personal data.

*CBPR*

The CBPR system is a framework designed to facilitate the secure and seamless flow of personal data across international borders while protecting individual privacy rights. It is intended to promote trust among participating economies, foster greater collaboration among data protection authorities, and provide a consistent set of standards and guidelines for companies that handle personal data.

Under the CBPR system, participating economies must establish their own national regulatory frameworks for data protection and privacy. These frameworks must be based on the principles and guidelines set forth in the APEC Privacy Framework. Companies that operate in these economies can participate in the CBPR system by voluntarily certifying that they meet the CBPR standards, by demonstrating compliance with the commonly agreed rules of 50 specific program requirements.

The CBPR system includes several key components, including a set of privacy principles that outline how personal data should be collected, used, disclosed, and protected. These principles include requirements for notice and consent, purpose limitation, data quality, and security safeguards. The CBPR system also includes a framework for accountability and enforcement, which includes mechanisms for dispute resolution and penalties for non-compliance.

CBPR offers benefits to organizations and participating economies in the following areas:

i. Facilitate cross-border personal data transfers: The CBPR system provides a standardized set of privacy principles and guidelines that facilitate the secure and seamless flow of personal data across international borders. This can help reduce barriers to trade and promote economic growth.

ii. Enhance trust and transparency: The CBPR system requires participating organizations to demonstrate their compliance with a set of internationally recognized privacy standards. This can help enhance trust and transparency between organizations, individuals, and participating economies.

iii. Provide a competitive advantage: Organizations that achieve CBPR certification can demonstrate their commitment to protecting individual privacy rights and may be perceived as more trustworthy and reliable than non-certified organizations. This can provide a competitive advantage in the marketplace.

iv. Improve data protection and privacy: The CBPR system requires participating organizations to implement robust data protection and privacy practices. This can help reduce the risk of data breaches, identity theft, and other privacy-related harms.

v. Promote collaboration and cooperation: The CBPR system encourages greater collaboration and cooperation among data protection authorities in participating economies. This can help improve the effectiveness and efficiency of regulatory oversight and enforcement.

vi. Support global privacy harmonization: The CBPR system provides a framework for the harmonization of privacy laws and regulations across participating economies. This can help reduce complexity and costs associated with compliance with multiple regulatory frameworks.

In particular, CBPR purports to bring several benefits to companies that participate in the system:

i. Enhanced privacy protection: The CBPR system requires companies to implement robust privacy policies and practices that are designed to protect personal data in accordance with established privacy principles. This can help build trust with customers and other stakeholders and reduce the risk of data breaches or other privacy-related incidents.

ii. Increased market access: Companies that achieve CBPR certification can demonstrate their commitment to privacy protections and international data flows, which can help them access new markets and customers that may require or value strong privacy protections.

iii. Simplified compliance: The CBPR system provides a consistent set of standards and guidelines for companies that handle personal data across multiple jurisdictions, which can

help simplify compliance and reduce the costs associated with navigating complex regulatory frameworks.

iv. Improved operational efficiency: The CBPR system provides a framework for companies to streamline their data management processes and reduce duplication and inefficiencies in complying with multiple data protection regulations across different jurisdictions.

# Key Observations

Despite the purported benefits of the CBPR, the participation of economies and companies in the system has been lacklustre. As of March 2023, there were 9 (out of 21) APEC economies participating in the CBPR, of which 5 economies had fully implemented the system in their jurisdictions with the appointment of Accountability Agents that can certify organisations have met the necessary requirements. There are slightly more than 60 companies in total that have been CBPR certified. There are several reasons that have contributed to the relatively low uptake of the Cross Border Privacy Rules (CBPR) system.

## (I) Limited awareness and understanding

The ABAC CBPR survey showed that slightly over half of respondents knew about the CBPR, reflecting that overall awareness of CBPR as a regional data privacy certification scheme was lower than optimal. Many organizations were simply not aware of the CBPR system or did not understand the benefits nor its requirements. This was particularly the case for MSMEs, which often lacked the resources and expertise to navigate complex regulatory frameworks.

## (II) Lack of incentive (business case)

There were no clear business-driven incentives for organizations to participate in the CBPR system as it remained unclear if the cost and effort required to comply with CBPR standards would outweigh the potential benefits of the certification.

*Limited value of CBPR to companies*

The participation by APEC economies was limited. Less than half of the 21 APEC economies had officially joined the APEC CBPR system. Of those 9, only 5 had taken the next step of designating Accountability Agents to conduct certifications. Other major economies in the Asia-Pacific had not indicated interest to participate in the CBPR. As such, businesses affirmed that the value of CBPR would increase with the number of economies participating in the system.

The value of the certification depended on whether it can legally be used as a data transfer mechanism. This required economies to amend their laws accordingly to recognise CBPR as an adequate mechanism. With only 60 over companies participating in the system, CBPR was not recognised or required as an adequate transfer mechanism amongst business-to-business (B2B) exchanges. The value of CBPR remained limited in so far until more economies recognised international privacy frameworks such as CBPR as a valid or adequate mechanism for international data transfer in their jurisdictions.

*Alternative Data Transfer Mechanisms*

With CBPR being one of the several data transfer mechanisms available, businesses did not need to rely on the CBPR or had little incentive to choose CBPR as their preferred mode of data transfers.

In the ABAC CBPR survey, 75% of respondents shared that they did not face challenges importing or exporting personal data across borders, given the alternatives available to facilitate the transfer of personal data across borders, with contractual agreements and binding corporate rules as the most frequently used mechanisms. Contractual agreements were seen to be more viable as they were shorter term endeavours that could be used to resolve the impetus to transfer data quickly. This is opposed to the CBPR certification, which was a longer-term endeavour for organisations, that often required strategic assessment and buy-in from the leadership team before embarking on such certifications. Nonetheless, companies acknowledged that having data privacy certifications had a positive impact on contractual negotiations, as such certifications served as a good base to start from, which made negotiations more straightforward, and helped to lower costs. Companies also noted that as rules on data privacy and governance get increasingly complex, the economies of scale could eventually tip in favour of certifications such as the CBPR which businesses can rely on as a to-go standard and basis of transfers in the future.

*Client Demand*

Client expectations were also a key factor in the decision-making process of attaining CBPR amongst companies. On customer demand, one company observed an increase in the number of clients requesting for CBPR as a requirement, particularly from Japan and Singapore. Another company shared that while it was contemplating to be CBPR certified, it eventually decided against it as it had assessed that demand from clients almost non-existent.

Relatedly, in discussing the merits of the CBPR, companies had also highlighted that the CBPR served dual functions as both a transfer mechanism and an accountability mechanism to demonstrate compliance to regional and global data protection standards. A CBPR-certified company attested to this, where the value of CBPR as a government endorsed, third-party certification had helped the company to demonstrate greater credibility and accountability in building their reputation as a trusted entity in various markets. This reflected the potential value add of the certification, where increased consumer education and client awareness could have a positive knock-on effect in increasing client expectations for businesses to be CBPR certified.

## (III) Fragmented Regulatory Landscape

The CBPR system is one of many types of data protection and privacy frameworks that exist in the world. This can inevitably create confusion and uncertainty for organizations that operate in multiple jurisdictions and may make it more challenging to achieve compliance with CBPR and other existing requirements.

*Regulatory Compliance*

It was no surprise that demonstrating accountability to regulators was top of mind amongst companies when assessing to be CBPR certified. Companies pointed out that the reality behind business motivation to proceed with such certifications were, more often than not, influenced by regulations, for e.g. the General Data Protection Regulation (GDPR) that imposed mandatory obligations onto any organisation, so long as the organisation targets or collects

data related to people in the European Union (EU). This brought to light the way in which compliance is traditionally perceived, i.e. from a defensive perspective, where attaining certifications and trust marks often stems from the need to ensure that an organisation is legally protected in the case of data breach incidents. As such, when adopting such lens, mechanisms such as the GDPR would make handling of disputes more straightforward. In comparison, the CBPR would appear to be less effective in such instances, when the value of the certification depends on the ability to use it as a legally recognised data transfer mechanism. Except for Japan, where CBPR is explicitly amended into its legislation, CBPR is not a mandatory requirement by regulators in other CBPR economies. In cases where certain privacy laws do not recognise international privacy frameworks such as CBPR as a valid or adequate mechanism for international data transfer, the CBPR's effectiveness is limited.

*Additional Enforcement Layer*

Companies also had concerns on whether having obtained CBPR certifications could make them subject to additional enforcement powers by the Accountability Agents. If so, this may be viewed as taking on additional legal risks and liabilities which are disproportionate to the benefits that a CBPR certification may give. In the event of non-compliance, the Accountability Agent had the power to enforce its program requirements against certified organizations and also had the power to refer the violation to the relevant public authority or privacy enforcement authority. The Accountability Agents could be private or government entities, and having a government entity as an Accountability Agent may be perceived by organizations as an additional regulatory layer for scrutiny.

## (IV) Differences in National Legislation

The CBPR system is based on the APEC Privacy Framework, which provides a set of high-level principles and guidelines for data protection. However, participating economies are also able to develop their own national laws and regulations that may differ from the CBPR. This could create additional complexity and uncertainty for organizations that operate in multiple jurisdictions.

Companies shared that there needed to be greater alignment between domestic privacy laws and CBPR to boost take up. Companies expressed that they were more likely to seek CBPR certification if CBPR could be used to demonstrate compliance with certain or several aspects of domestic privacy laws. Streamlining compliance and certification processes where possible would allow companies to save significant manpower, resources, and compliance related costs. In the absence of that, companies would inevitably prioritise meeting domestic requirements over CBPR or any other privacy certifications to be able to operate without any restrictions in-market. In addition, companies also pointed out that a CBPR certification may not necessarily reduce obligations under existing domestic laws. This would mean that where local data privacy requirements are more onerous than CBPR's common baseline standards, additional requirements applicable under local law would still need to be complied with. Hence, businesses that have obtained CBPR certification would still need to invest adequate resources to ensure that there is compliance to both.

In such instances, MSMEs would seldom have an option to consider applying for CBPR. A firm that assists clients to attain certifications attested to this, in that its MSME customers prioritised obtaining the local trust mark even though CBPR certification was offered together as a package during application. It was apparent that given the limited time and resources of MSMEs, they had to focus on what was necessary, and not what was a good-to-have.

Nonetheless, companies also recognised that the CBPR cannot replace domestic legislation altogether as the latter's scope and areas of coverage go beyond the CBPR. While the CBPR only governs and certifies the requirements needed for the transfer of data overseas, domestic regimes include requirements on how you handle, control and process data domestically even before it is ready for cross border transfers. As such, domestic privacy legislation remained important.

## (V) Lack of Global Access and Inclusivity

Large corporations took a globalist perspective on the applicability of the CBPR, i.e. studying considerations on how CBPR would be operationalised across the supply chain. Relatedly, a large company shared its challenges to appoint a suitable Accountability Agent who would be able to certify an organisation of its size and scope, given an inherently complex internal corporate structure, quantity and speed in which data is stored, processed, and transferred, the employment of a significant number of local subcontractors, and geographical span of operations in several economies across the world, beyond the APEC region. As such, the company cautioned on the difference in costs and resource commitments on its end, where the certification and renewal process of the CBPR for such companies could take up to 6 months.

To ensure that all players in the supply chain were incorporated into the CBPR system, fundamental questions arose on what needed to be done to ensure that the CBPR was accessible to all types of businesses, especially MSMEs. The scalability of the CBPR on a global level had to be considered seriously. One, it was clear that MSMEs were at a disadvantage and not best placed to benefit from the certification, given the high barriers of entry and continuity. Two, it was important to recognise that most economies in the world are at different stages of economic growth and development, with many developing economies having scarce or non-existent data privacy laws in place. Hence, there was a need to take a step back to focus on the development of government officials and regulators in data protection competencies and create greater awareness amongst local enterprises in developing economies on the importance and benefits of good data privacy practices. It became clear that to promote greater global access and inclusivity of the CBPR, scalability of the CBPR (via capabilities development of government and industry) needed to be prioritised in economies where privacy legislation is scarce.

# Recommendations

Given the impediments and concerns that businesses grapple with when assessing the value of the CBPR certification, improving uptake of the CBPR system will require a concerted multi-stakeholder effort from governments, industry, and others such as academia, non-governmental organisations and civil society to address the gaps and challenges that exist around awareness, access and affordability, harmonisation and interoperability to expand participation across economies and the business community.

The industry converged on 4 key areas that needed to be tackled to boost uptake of the Cross Border Privacy Rules (CBPR) system:

## (I) Expanding CBPR Participation

Efforts should be made to encourage more economies (APEC and non-APEC) to participate and implement the CBPR system. With more economies recognising the CBPR as a valid data transfer mechanism under local jurisdictions, the value and impact of the CBPR certification would increase substantially. This would also eventually result in greater trust and collaboration amongst participating economies in the privacy space. Specifically, companies expressed interest to see ASEAN, EU, Middle East and Latin American economies' participation.

In that regard, companies recognised that the move for the CBPR to be expanded from APEC to being a global system is a step in the right direction, given that the digital economy is not defined or constrained to one region. Companies believed that the set of principles and guidelines set out under the APEC Privacy Framework would benefit regions and economies beyond the Asia-Pacific, in allowing for greater harmonisation of the personal data transfer landscape between regions, and to raise the overall global norms and standards governing cross border personal data transfers.

Getting more economies onboard would also require having serious conversations around data localisation and the need to shift mindsets in order for governments, law makers and communities to see the merits on how freer flows of data can result in greater economic prosperity. Companies recognised that facilitating discussions at the government-to-government (G2G) level would not suffice and require active business-to-government (B2G) engagements as well to supplement the commercial impetus for CBPR participation.

Companies were also of the view that as a next step, it would be worthwhile to focus efforts to build capabilities and awareness within the existing 9 economies and businesses operating in these jurisdictions to build a sizeable pool of CBPR-certified companies in the ecosystem. This could spur a knock-on, domino effect of an increased demand for the certification.

## (II) Building Awareness & Education

Efforts should be made to increase awareness and understanding of the CBPR system at various levels. With governments and regulators, dialogue is necessary both at the G2G level to socialise the merits of CBPR as a government-backed certification to meet governments' data protection needs, and at the B2G levels to articulate the commercial value that CBPR

brings to businesses, be it the potential cost savings, compliance benefits and increased credibility of organisations.

For businesses, there needs to be active G2B engagement via broad-based awareness building sessions and targeted education across various segments and sectors of industries to articulate the value of CBPR to companies. As a government-backed certification, it is key for governments to send a strong signal to industry to get behind the CBPR. In that regard, there also needs to be regular engagement points where the private sector can engage with regulators and other stakeholders to provide feedback on the CBPR system and help identify areas for improvement. This can help ensure that the CBPR system remains relevant and effective in meeting the needs of organizations and individuals.

Most importantly, there needs to be a strong business case to increase uptake. To successfully market CBPR, one way could be to identify organisations that are already certified or in the process of certification to champion advocacy amongst their sector and peers. The promotion of use cases and tangible benefits of obtaining the certification could help generate greater demand amongst clients, consumers and corporate partners within business networks to be certified. This can help build momentum for greater uptake of the CBPR system among other organizations and stakeholders.

## (III) Increasing Accessibility & Inclusivity

For large companies and groups of companies that operate in numerous economies, harnessing the full potential of being CBPR certified would also mean that they need to be able to get their sub-contractors to attain the certification. As such, some work needs to be done in this aspect to ensure that the entire supply chain is gradually incorporated into the high standards of compliance and dealing with personal data.

There is also a need to make the CBPR more accessible to MSMEs that will naturally struggle to meet the requirements, navigate the assessment, attain certification, perform the necessaries for annual renewal, etc. There is a need to engage academia and civil society in the discourse to help plug these gaps, i.e. to increase awareness and accessibility to the requirements and meeting such requirements, help shift cultural expectations of privacy regimes specific to domestic law and context in economies, etc.

Making the CBPR system more accessible to MSMEs will require a concerted effort by stakeholders, including governments, industry associations, civil society and other private sector organizations. Simplifying the certification process, providing training and support, increasing awareness, providing financial assistance, and developing alternative certification models are all potential strategies to help make the CBPR system more accessible to MSMEs.

i. Simplify the certification process: The CBPR system certification process can be complex and expensive, making it difficult for MSMEs to participate. Simplifying the certification process and reducing the associated costs can make it more accessible to MSMEs.

ii. Provide training and support: MSMEs may lack the resources and expertise to navigate the CBPR certification process. Providing training and support on the requirements for certification, and offering tools and resources to help with compliance, can make it easier for MSMEs to participate.

iii. Increase awareness: Many MSMEs may not be aware of the CBPR system and the benefits of certification. Increasing awareness of the program and its benefits through targeted outreach and marketing efforts can help encourage greater participation.

iv. Provide financial assistance: MSMEs may face financial barriers to participation in the CBPR system. Providing financial assistance, such as grants or low-interest loans, can help reduce these barriers and make participation more accessible.

v. Develop alternative certification models: Alternative certification models that are tailored to the needs of MSMEs can make it easier for them to participate in the CBPR system. For example, group certifications or self-assessment programs may be more suitable for smaller organizations.

## (IV) Promoting Harmonisation, Mutual Recognition and Interoperability

In the process of expanding the CBPR system to be more inclusive, companies also noted that it would be critical to ensure that both the APEC and Global CBPR systems remain aligned to prevent further fragmentation and increased complexity of data governance. In that regard, certification on either system should allow for mutual recognition to ensure that both mechanisms remain complementary. It was key that the spirit to expand the system to include all economies and businesses in the world remained as the core interest, and the purported benefits of the CBPR to harmonise data privacy regulations to facilitate increased, and seamless cross border data flows remains as the priority and goal to aspire to.

Efforts need to be taken to promote greater harmonisation of data protection and privacy laws and regulations across participating economies. This could help to greatly reduce the complexity and costs associated with compliance with multiple regulatory frameworks.

At present, there is no global interoperability between the various data transfer mechanisms. For businesses that must transfer data globally, a cost-benefit analysis needs to be undertaken to review compliance vis-à-vis various transfer mechanisms. Therefore, it is worth considering ways to increase CBPR's interoperability as a widely recognized instrument for cross-border data transfers with other APEC and non-APEC economies' privacy frameworks, including the GDPR and frameworks prevalent in the Middle East and Africa regions. The value of the CBPR certification is only set to increase as more economies recognise it as an adequate transfer mechanism.

Streamlining parts of local compliance requirements with CBPR promotes harmonisation and serves as incentive to businesses in being able to demonstrate partial or full compliance with local laws if they have obtained a CBPR certification. The CBPR program requirements align with key aspects of most data protection laws. Therefore, a company that obtains CBPR certification could be deemed to be in compliance with some domestic legal requirements. Local data protection authorities would also benefit from recognizing CBPR certification as a sign of compliance as it would allow them to focus their enforcement resources on companies that have not demonstrated compliance with CBPR or other certification requirements.

# Conclusion

The CBPR system has the potential to enhance privacy protections, promote regulatory cooperation, provide a competitive advantage, support innovation, and simplify compliance for organizations that operate across international borders.

Improving CBPR uptake requires strong and sustained multi-stakeholder partnerships. The private sector can play an important role in promoting the uptake of the CBPR system by advocating for participation, providing training and support, encouraging harmonization, participating in pilot programs, and engaging with regulators and other stakeholders. There also needs to be an open avenue for regular, robust dialogue between government, industry, academia and civil society to develop targeted action plans and initiatives.

International advocacy platforms such as ABAC and industry associations could play a particularly beneficial role in serving as the bridge to facilitate partnerships and dialogue between government and industry. These platforms and associations could help to coordinate and steer stakeholders in the right direction to operationalize recommendations and next steps.

To move the needle, there needs to be both general awareness campaigns, and regular closed-door, focused group consultations and capacity building initiatives with governments and business communities. These sessions could focus on identifying and tackling specific challenges step-by-step that need to be overcome, and the capabilities and functions that need to be established and integrated to improve current privacy regimes. These sessions would be most effective and yield maximum results if they are incorporated as formal taskforces or action plans that are resourced and endorsed by the highest level of stakeholders in governments, business communities, educational bodies, and relevant non-governmental organisations.

# About SGTech

SGTech, celebrating its 40th anniversary in 2022, is the leading trade association for Singapore's tech industry. Representing over 1,000 member companies ranging from top multinational corporations, large local enterprises, vibrant small and medium-sized enterprises, and innovative startups, it is the largest community in Singapore where companies converge to advocate for change and drive what enables tech innovation and accelerates tech adoption to spur greater sustainability in the sector.
SGTech's mission is to catalyse a thriving ecosystem that powers Singapore as a global tech powerhouse.

SGTech's initiatives are guided by two strategic thrusts:

- To position Singapore as a global node for digital and data, built on trust.
- To inspire the tech sector to take collective action and be part of the sustainability solution in Singapore and globally

Underpinning these two pillars, and all our business activities, is our continuous drive for Talent for Tech.

Learn more from our website